Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

Specification Amendments

Replace the paragraph between lines 20-25 on page 1 of the specification with the following:

--With the increasing advent of cashless payment traffic and the ~~increasing information technological networking as far as into~~ increase of information network-technology even in individual households, such as e.g. in case of pay TV applications, there is an increasing demand for cryptographic algorithms in order to be able to perform digital signatures, authentications and encryption tasks. Known cryptographic algorithms comprise asymmetric encryption algorithms, such as e.g. the RSA algorithm, symmetric encryption processes, such as e.g. the [[DSE]] DES process, as well as processes based on elliptic curves.--

Replace the paragraph between page 2, line 30 and page 3, line 18 of the specification with the following:

--For protecting chip card terminal systems against criminal manipulations, specific protocols are employed between terminal and chip card, comprising e.g. mutual authentication as well as encryption and decryption operations making use of

the cryptographic algorithms implemented in the cryptographic processor. A problem with conventional chip cards consists in that the algorithms used for the secret functions, e.g. for encryption, are fixedly provided on the chip card in the form of a fixed wiring and/or in stored form and thus are susceptible to being spied out by potential attackers. Spying out of cryptographic algorithms implemented in chip cards by an attacker comprises, for example, the chemical removal of the circuit structure of the cryptographic processor and the optical analysis of the exposed semiconductor structures. If an attacker, by way of the chip card in his possession, succeeds in obtaining the cryptographic algorithm implemented therein, the attacker will be in the position, due to his knowledge of the cryptographic algorithm and thus by the possibility of implementing the same, to carry out certain attacks against the chip card in order to obtain the secret data, such as the secret key or other data of crucial security of the chip card. When the underlying cryptographic algorithm is known, the attacks have a [[by]] far greater chance of success, and consequently the security chain of the chip card traffic is at risk.--

Replace the paragraph between lines 20-34 on page 3 of the specification with the following:

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

--With conventional chip cards, the problem of spying out is counteracted merely by specific hardware processes or technologies, such as by the hidden contact process. In case of this process, attempts are made to prevent the optical analysis of removed semiconductor structures and thus a conclusion to the underlying electronic circuit by means of hidden contacts and by the use of specific layout libraries for the underlying gates, in which different gates, such as AND gates and OR gates, differ from each other merely by different doping. These hardware concealing measures indeed increase the expenditure for finding out the underlying cryptographic algorithms for the potential attacker, but on the other hand also increase ~~also~~ the circuitry and design expenditure, the chip area and thus the costs of the cryptographic processor and the chip card, respectively.--

Replace the paragraph between lines 14-29 on page 4 of the specification with the following:

-- In accordance with a first ~~aspect~~ object of the invention, this ~~aspect~~ object is achieved by a security module for use with a terminal, comprising a data interface adapted to be coupled to a terminal, for receiving at least part of an algorithm code or of the complete algorithm code from the

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

terminal, with the algorithm code concerning a processing of

secrets,

an ~~energy~~ power interface for receiving supply ~~energy~~ power

from the terminal; a volatile memory for storing the part of

the algorithm code or the complete algorithm code received via

the data interface, said volatile memory being coupled to the

~~energy~~ power interface in order to have ~~energy~~ power supplied

thereto such that the same will be cleared upon an

interruption of the receipt of the supply ~~energy~~ power from

the terminal; and a processor for performing the algorithm

code in order to obtain an algorithm code result that can be

delivered to the terminal.--

Replace the paragraph between page 4, line 31 and page 5, line

13 of the specification with the following:

-- In accordance with a second ~~aspect~~ object of the invention,

this ~~aspect~~ object is achieved by a terminal for use with a

security module, comprising: a data interface adapted to be

coupled to the security module, for transmitting at least part

of an algorithm code or the complete algorithm code from the

terminal to a volatile memory of the security module and for

receiving the algorithm code result from the security module,

with the algorithm code concerning a processing of secrets;

and ~~an energy~~ a power interface for delivering supply ~~energy~~

5 of 41

PAGE 5/41 * RCVD AT 7/10/2007 3:56:47 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/14 * DNIS:2738300 * CSID:9549251101 * DURATION (mm-ss):10-00

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

power to the security module, with the volatile memory being

supplied by the supply ~~energy~~ power, such that the same will

be cleared upon an interruption of the receipt of the supply

~~energy~~ power from the terminal, with the terminal, for each

communication operation between terminal and security module

during one and the same communication operation with the

security module, being designated to send at least the part of

the algorithm code or the complete algorithm code to the

volatile memory of the security module; and, subsequently,

during the further communication process, receive the

algorithm code result from the security module.--

Replace the paragraph between lines 15-31 on page 5 of the

specification with the following:

--In accordance with a third ~~aspect~~ object of the invention,

this ~~aspect~~ object is achieved by a process for computing an

algorithm code result using a security module, comprising the

steps of: receiving at least part of an algorithm code or the

complete algorithm code by means of an ~~energy~~ interface, with

the algorithm code concerning a processing of secrets;

volatile-storing said part of the algorithm code or said

complete algorithm code in a volatile memory of the security

module, with the volatile memory being coupled to the ~~energy~~

interface, to be supplied with ~~energy~~ power, such that the

PAGE 6/41 * RCVD AT 7/10/2007 3:56:47 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/14 * DNIS:2738300 * CSID:9549251101 * DURATION (mm-ss):10-00

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

from the terminal; and receiving the algorithm code result

from the security module.--

Replace the paragraph between lines 13-28 on page 6 of the

specification with the following:

--In accordance with a fifth ~~aspect~~ object of the invention,

this ~~aspect~~ object is achieved by a process for communication

between a security module and a terminal, comprising the steps

of: transferring at least part of an algorithm code or the

complete algorithm code from the terminal to the security

module, with the algorithm code concerning a processing of

secrets; volatile-storing said part of the algorithm code or

said complete algorithm code in a volatile memory of the

security module, with the volatile memory being supplied by

the supply ~~energy~~ power, such that the same will be cleared

upon interruption of the receipt of the supply ~~energy~~ power

from the terminal; performing said algorithm code on the

security module in order to obtain an algorithm code result;

delivering said algorithm code result to the terminal; and

clearing said volatile memory upon an interruption of the

receipt of the supply ~~energy~~ power from the terminal.--

Replace the paragraph between lines 18-38 on page 7 of the

specification with the following:

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

--According to the invention, a security module, such as a
chip card, comprises a TPM (Trusted Platform Module) in the
form of a computer plug-in module or a smart card, for use
with a terminal in addition to a data interface adapted to be
coupled to the terminal and receiving from the terminal at
least part of the algorithm code or the complete algorithm
code, ~~an energy~~ a power interface receiving supply ~~energy~~
power, as well as a volatile memory for storing the part of
the algorithm code received via the data interface or of the
complete algorithm code received, with the volatile memory
being coupled to the ~~energy~~ power interface in order to have
~~energy~~ power supplied thereto. A processor performs the
algorithm code in order to obtain an algorithm code result
that can be delivered to the terminal. The ~~not received~~
remainder of the algorithm code not having been received may
be stored, for example, in a non-volatile memory, such as a
ROM, of the security module. If there is not sufficient supply
~~energy~~ power present, there is thus no complete algorithm code
contained in the non-volatile memory of the security module,
and consequently there is no complete algorithm code available
to be run by a potential attacker.--

Replace the paragraph between page 7, line 40 and page 8, line
13 of the specification with the following:

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

--A terminal suitable for use with the security module

described hereinbefore, such as e.g. an automatic cash

dispenser, a mobile telephone with card reader, a pay TV

decoder or a computer having a plug-in place for a TPM,

comprises for example a data interface that is adapted to be

coupled to the security module and transmits the part of the

algorithm code or the complete algorithm code from the

terminal to the volatile memory of the security module and

receives the algorithm code result from the security module,

as well as ~~an energy~~ a power interface delivering the supply

~~energy~~ power to the security module.--

Replace the paragraph between page 8, line 15 and page 9, line

8 of the specification with the following:

-- According to a specific embodiment, an authentication, such

as an authentication according to the challenge and response

scheme, is carried out between the terminal and the security

module during a communication between terminal and security

module. The transfer of the algorithm code from the terminal

to the security module is carried out in encrypted and

certified form in order to counteract eavesdropping and

manipulation of the communication connection between terminal

and security module. The terminal or the security module to

10 of 41

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

this end contains suitable means for performing

authentication, encryption and decryption as well as

certification and certification examination, respectively. For

increased security and for effectively preventing access of a

potential attacker to the transferred part of the algorithm

code, the security module may have in addition a monitoring

means which, if predetermined security conditions are

fulfilled, clears the volatile memory. Such security

conditions may comprise the interruption, an irregularity and

a fluctuation in the supply voltage and/or the processor or

system clock or other operating parameters as they may be

effected by manipulation of the security module while the

latter interacts with the terminal. In the event that the

monitoring means has not effected preliminary clearing of the

memory, the volatile memory and thus the part stored of the

algorithm code is cleared at the latest upon termination of

the communication between terminal and security module or upon

interruption of the supply ~~energy~~ power, respectively, such as

e.g. by withdrawal or removal of the security module from the

terminal, whereby this part of the algorithm code is no longer

available to a potential attacker for ~~performing in the scope~~

~~of~~ being run within specific attacks.--

Replace the paragraph between lines 10-24 on page 9 of the

specification with the following:

11 of 41

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

-- In order to further reduce the attackability of the system,
it may be provided to transfer the part of the algorithm code
from the terminal to the security module intermittently in
modified form and repeatedly and, in doing so, to store each
time the newly transferred, altered part of the algorithm code
in the volatile memory instead of the old stored part of the
algorithm code. This renders possible changes in a
cryptographic algorithm during the communication between
terminal and security module, such as e.g. in case of pay TV
applications, but also changes in the algorithm code each time
upon initialization of a terminal-security module
communication, such as e.g. in case of credit cards, whereby
it is further aggravated for a potential attacker to ~~adjust~~
~~to, or~~ find out [[,]] the algorithm code employed.--

Replace the paragraph between page 9, line 26 and page 10,
line 13 of the specification with the following:

--In addition to protecting the algorithm code of the security
module against spying out by a potential attacker, an
additional advantage of the present invention consists in that
it is applicable to a multiplicity of application fields, such
as e.g. EC (Electronic Cash) cards, credit cards, multi-
application cards or pay TV smart cards. Depending on the

particular application, the algorithm code or security

function code received by the security module contains parts

of a code for functions of crucial security or one or more

cryptographic algorithms of the security module. For chip card

producers or producers of security modules, the versatile

applicability as well as the enhanced security against

potential attacks means increased acceptance in the market and

thus an increased market share. In addition thereto, the

security of the security module is increased in inexpensive

manner as the increased security is achieved by software

loading of the volatile memory. The conventional and complex

hardware measures for protecting the algorithm code against

potential attackers, as described hereinbefore, may either be

carried out in addition or be replaced by less expensive

hardware techniques since the functions of crucial security or

the underlying cryptographic algorithm of the security module

are not permanently provided on the chip card.--

Replace the paragraph between page 10, line 38 and page 11,

line 15 of the specification with the following:

-- It is pointed out that the following detailed description

of specific embodiments of the present invention refers to

chip card applications by way of example only, and that the

present invention is also applicable to other security

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

modules, such as TPMs in the form of plug-in ~~cards~~ boards; the

following description may easily be transferred to such

applications. Accordingly, the following description also

refers to terminals for chip cards, such as e.g. cash

dispensing machines, by way of example only, although a

terminal according to the present invention, in other fields

of application, may also be a computer, for example, having a

TPM in the plug-in ~~spaces~~ slots thereof, or a mobile telephone

with a smart card in the card reader thereof, or the terminal

may generally be an arbitrary apparatus capable of

communicating with the security module.--

Replace the paragraph between page 11, line 38 and page 12,

line 15 of the specification with the following:

--The steps illustrated in Fig. 1 have the prerequisite that a

communication is already possible between the terminal and the

chip card which, for example, may be the case upon

introduction of the chip card into the terminal; in this

regard, the terminal 20 may be a contactless or contact

terminal, and the communication connection thus may take place

without contact or via a contact. It is necessary furthermore

for communication that chip card 10 be supplied with ~~energy~~

power from terminal 20, which may also be carried out in

contactless manner via electromagnetic radiation or via a

14 of 41

contact. After the communication connection between terminal

20 and chip chard 10 has been established and supply ~~energy~~

power has been supplied to chip card 10, initializing steps

may be carried out first, such as e.g. the mutual agreement on

the relevant protocol etc.--

Replace the paragraph between lines 17-36 on page 12 of the

specification with the following:

-- After the steps (not shown) of supplying ~~energy~~ **power** to

the chip card 10, establishing the communication connection as

well as initializing the communication between terminal 20 and

chip card 10, mutual authentication between terminal 20 and

chip card 10 is carried out in a step 30, e.g. an

authentication in accordance with the challenge and response

process. The mutual authentication may comprise, for example,

the inputting of a PIN (Personal Identification Number) by the

card user, in which the mutual authentication 30 makes use,

for example, of chip card-specific data stored on the chip

card 10, such as e.g. a chip card identification number and a

personal identification number, in connection with a chip card

key stored on the chip card as well as an authentication code

stored on the chip card and representing a cryptographic

algorithm, such as e.g. a symmetric or an asymmetric

cryptographic algorithm. The authentication serves to make

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

sure that only admitted chip cards may communicate with

admitted terminals. If the authentication yields an error, the

communication connection is terminated.--

Replace the paragraph between lines 22-32 on page 13 of the

specification with the following:

-- In case the certificate examination reveals that the

certificate lacks genuineness, the communication between

terminal 20 and chip card 10 is interrupted, and there may be

provisions made that the chip card 10 ~~does not~~ longer ~~carry~~

~~out processings~~ operates for a predetermined period of time.

It is thus avoided that a potential attacker taps the

communication connection between terminal 20 and chip card 10

and enters a "false" code to the volatile memory of the chip

card 10 which, upon performing by the chip card 10, could

effect the outputting of secret data stored on chip card 10,

for example.--

Replace the paragraph between page 13, line 34 and page 14,

line 21 of the specification with the following:

-- If the certificate examination revealed the genuineness of

the certificate, the transferred part of the algorithm code is

then stored, in a step 50, in a volatile memory of chip card

10 either in encrypted or in decrypted form. Depending on encrypted or decrypted storage, the algorithm code is decrypted before storage thereof or before ~~performing~~ execution by a cryptographic processor on chip card 10. The algorithm code having a part thereof transferred in step 40 may comprise the program code of one or a plurality of functions of crucial security of the chip card 10, such as e.g. a debiting or crediting function for charging or discharging the chip card 10, or the program code for performing a cryptographic algorithm necessary during the further communication sequence, such as e.g. a symmetric or asymmetric cryptographic process, an RSA algorithm, encryption according to the DES ~~standard~~, an elliptic curve process or another secret algorithm, however without restriction to these examples. In the event of a pay TV application, the algorithm code comprises, for example, information with respect to decryption of the television data of a chargeable program, such as e.g. the repermutation of the image lines of an image of the television data. Consequently, the algorithm code to be protected is present in complete form on chip card 10 only during the time of execution of the communication between terminal 20 and chip card 10.--

Replace the paragraph between page 14, line 39 and page 15, line 27 of the specification with the following:

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

-- In a step 70, the part of the algorithm code stored in the

volatile memory is cleared again. Clearing of the algorithm

code may be effected, for example, by taking out the chip card

10 from terminal 10 by the card user and by thus interrupting

the delivery of supply ~~energy~~ power from terminal 20 to chip

card 10. ~~For preventing attempts of~~ In order to prevent

potential attackers ~~to protect~~ from protecting the volatile

memory, e.g. a RAM, ~~against loss of~~ from loosing the stored

part of the algorithm code[[,]] (whereby -if successful, these

would come into possession of the complete algorithm code),

the chip card 10 may have a specific monitoring means provided

thereon which effects active clearing of the volatile memory

of the chip card 10 also ~~if~~ in case a monitoring operation

reveals that specific security conditions are fulfilled, such

as interruption of the system clock, the interruption of the

delivery of supply ~~energy~~ power or other indications for a

possible attack, such as voltage fluctuations or the like.

Consequently, the algorithm code, after utilization of the

chip card 10 in the terminal 20 or interference with the

communication sequence, is no longer present on chip card 10

and thus is no longer exposed either to potential attacks and

spying out by potential attackers. An attacker in possession

of the chip card cannot carry out security computations on the

basis of the complete algorithm code since the latter is not

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

completely in the range of access of the attacker. The spying

out of keys or algorithms is thus effectively prevented.--

Replace the paragraph between lines 18-35 on page 17 of the

specification with the following:

-- With reference to Fig. 2 and Fig. 3, possible embodiments

for the construction of a chip card and a terminal,

respectively, will be described hereinafter. Fig. 2 shows a

block diagram of a chip card generally designated 100. Chip

card 100 comprises a data interface 110, an energy a power

interface 120, a RAM 130, a processor 140 and a ROM 150. The

data interface 110 is adapted to be coupled to a terminal (not

shown) for example via a contactless coupling or via a contact

and is capable of transmitting data from the chip card to the

terminal and, vice versa, of receiving data from the terminal.

The data interface 110 is connected to processor 140 whereby

the data to be transmitted and received can be transmitted to

and from processor 140, respectively. The energy power

interface 120 is adapted to be coupled to the terminal as well

in order to obtain from the terminal supply energy power in

the form of, for example, electromagnetic energy power or a

supply voltage. Energy Power interface 120 distributes the

supply energy power to the processor 140 and the RAM 130.--

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

Replace the paragraph between page 18, line 37 and page 19,

line 19 of the specification with the following:

--Fig. 3 shows a block diagram illustrating the terminal

construction in accordance with an embodiment of the present

invention. The terminal, generally designated 200, comprises a

data interface 210, an ~~energy~~ power interface 220, a processor

230 connected to data interface 210 and ~~energy~~ power interface

220, as well as a memory 240 connected to processor 230. The

data interface 210 is adapted to be coupled to the data

interface of a corresponding chip card in order to carry out a

data exchange between the terminal 200 and the chip card (not

shown). The ~~energy~~ power interface 220 is also adapted to be

coupled to an ~~energy~~ power interface of the particular chip

card in order to deliver supply ~~energy~~ power thereto.

Processor 230 controls, for example, the sequence of

operations during communication of terminal 200 with the chip

card and performs, for example, the initialization,

authentication, the encryption of the algorithm code to be

transferred, which is stored in memory 240, the certification

thereof as well as the transfer of the encrypted and certified

algorithm code to the data interface 210 for transfer thereof

to the chip card.--

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

Replace the paragraph between page 19, line 27 and page 20,

line 7 of the specification with the following:

-- With respect to the preceding description, it is pointed

out that the same has referred to specific embodiments only.

The mutual authentication and the encryption of the part

transferred of the algorithm code as well as the certification

may be omitted in specific applications, for example. Due to

the very measure according to the invention, that at least

part of the algorithm code is stored in a volatile memory of

the chip card, it is rendered very difficult for a potential

attacker to perform functions of crucial security of the chip

card, such as e.g. encryption algorithms and access functions

to chip card specific information, such as a balance etc.,

since these are not permanently stored on the chip card and

thus are not in the possession of the potential attacker, but

rather are lost if supply ~~energy~~ power is no longer received.

The attempt of protecting the volatile memory against loss of

this function turns out to be very difficult and may be deemed

to be not realizable in practical application. --

Replace the paragraph between lines 20-37 on page 20 of the

specification with the following:

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

-- A current possibility of realization of the present

invention consists, for example, in the processor of product

family SLE66CX320P of the company Infineon AG, which by way of

an MMU (MMU = Memory Management Unit) renders possible to run

a code stored in a RAM in that it controls memory access

operations to the RAM. In the simplest case, ~~already~~ even the

transfer of only encrypted jump addresses or memory addresses

from the terminal to the chip card would effectively prevent

that a "native code" or machine code can be loaded by a

potential attacker. ~~Already~~ Even with such a simple

realization of the present invention, an attacker would not be

able to perform the security computations in the chip card,

since the jump addresses and thus the sequences would be

unknown. This idea may be imparted to a customer of such a

component by drafting an application note, thereby increasing

the security of the application with corresponding realization

thereof in the controller software of the chip card and in the

terminal software.--

Replace the abstract of the disclosure with the following:

-- A security module for use with a terminal comprises a data

interface adapted to be coupled to a terminal, for receiving

at least part of an algorithm code or the complete algorithm

code from the terminal, as well as an ~~energy~~ power interface

22 of 41

Applic. No. 10/620,108
Amdt. dated July 10, 2007
Reply to Office action of April 10, 2007

for receiving supply ~~energy~~ power. A volatile memory coupled to the ~~energy~~ power interface in order to have ~~energy~~ power supplied thereto stores the part of the algorithm code or the complete algorithm code received via the data interface, with a processor performing the algorithm code in order to obtain an algorithm code result that can be delivered to the terminal. Due to the storing of at least part of an algorithm code in the volatile ~~memoryof~~ memory of the security module, according to the invention, the algorithm code of the security module is effectively protected against spying out by a potential attacker.--

~~Fig. 2~~--